Privacy Awareness Week 2024 Launch

Kim Skubris:

Well good morning, everybody, and welcome after a long weekend, Queenslanders do it well, to our Privacy Awareness Week launch for 2024. My name is Kim Skubris and I'm absolutely delighted to be invited by the Office of Information Commissioner to once again be your event host, as we look to privacy today through the technological lens. We look through security, accountability and accessibility and as someone who for 30 odd years as a broadcast journalist with the Seven Network, needless to say story telling is my passion. And today you're going to hear some thought-provoking yarns. Some of you might be trying to do the math, and I like to say Chanel 7 was hiring cadets at the age of 12, but in the spirit of privacy, I'm going to keep my age under wraps. I live in Brissie with my three children, aged 13, 16 and 52, and when my 13-year-old this morning said, mum, you know, what's this big deal about, you know, getting information, everything's cashless, tap and go. I said yeah, let's have a think about that. So I'd like to start this morning by sharing a story myself.

Last week in Sydney heavily armed police officers stormed a home in Fairfield and they arrested a 46-year-old man who consequently was charged with blackmail. The arrest was the result of a website which was discovered by detectives and had no less than the personal information of more than one million patrons who were accessing and enjoying clubs across New South Wales. Now in the media game we have a saying; facts tell, stories sell. The fact of the matter is, the fact is, this is concerning. Concerning was the word that was used over and over again by presidents of clubs, from bowling, to surf clubs and so forth. But when you consider it, and in my experience over the past, as I said, 30-odd years, when you throw really big numbers at an audience, we can say that they can wash over you. But when I thought about that, one million patrons, you know who I thought about? My mum and dad.

Now my mum will have my behind if I say my elderly parents, but she is 79, so is dad. And I'd just like to share that when I think about them going to the surf club, and innocently and with trust handing over their driver's licence or getting facial recognition, because they're doing the right thing, it really gets my goat that they could then unwittingly be the target of a scammer. Because now more than one million people in Australia, patrons just like my mum and dad, are being contacted by clubs saying be on alert. And we all need to be on alert and we're going to hear more about that today. As I've welcomed all of you, I'd also like to welcome everyone who's joining us from across Australia. Privacy and Information Commissioners, Ombudsmen and staff, and welcome to, as I said, Brisbane's launch of privacy awareness week. And in that vein, I would now sincerely like to acknowledge the Traditional Owners of the land in which we gather, the Turrbal and Jagera People, and pay my respects to Elders past, present and emerging. And it is my pleasure to introduce to you, if you don't know him already, Uncle Billy Cummings, who is here with the blessing of one of my favourites, Songwoman Maroochy. Uncle Billy, thank you for coming and sharing with us today. Welcome to Country. Thank you.

Uncle Billy Cummings:

(Speaker speaks in Aboriginal language).

I said welcome, welcome, welcome. Usually, we'll have you walk through some smoke and we believe that smoke keeps out, stops negativity from coming into our camp, bad [unintelligible –

“(ui)”] or bad spirts, bad (ui), and only good come through. I said (ui), means my mother, which you refer to as the earth. Because for thousands and thousands of years our mother, like your mothers, have provided you with, when you were little, something to drink, something to eat, nurture you when you are sick, shelter you, keep you safe. That’s why we get a bit annoyed at destruction that’s going on because it’s making our mothers sick, it’s also your mother too, and if she get really sick, you know what, everybody gets sick, and you can't turn back. We know these stories from our old ancient people, before the Barrier Reef was even here, when dinosaurs roamed. There’s a, wombat, youse know what wombats, how big they are today? There's a fossil of a wombat there. Our people used to hunt, they're three times the size of a cow back then. Kangaroos, 16, 14 foot tall. And all over this land a child was born, no matter where you go in this country. A barma(?) child, barma means human being. That’s what we refer to each other in language. (Ui) barma, I said what's happening, where you going, human being? These languages are still with us as our customs. I said Milperra, big strong powerful spirit that swims up and down the Brisbane River looking over all the surrounding clans, making sure that all the laws from the first light adhered to and the first law from our first light is respect, caring and sharing for each other. So (ui)... when I said (ui), that’s what I referred to, we refer to as non-Aboriginal people. But we all share this country today and so should we share our traditional laws where we are (ui) Meeanjin, youse call it Brisbane, its real name is Meeanjin (?). From dreamtime we should be, everybody should be adhering to respect, caring and sharing. Of course, we’re not going to stop developments and all that, but we can slow it down and look at each other more closely and talk. Truth telling has been hidden for a long time. So welcome, welcome, welcome, enjoy your conference and thank you to organisers for the acknowledgement and respect. Me, (ui) saying thank you from the Yuggera and Turrbal people, and thank you again. Have a good day.

Applause

Kim Skubris:

Thank you so much, Uncle Billy. And we are going to stop today, and we are going to chat today, and those of you who know my hosting style, I don’t insult your intelligence, you're all highly intelligent people. If you can't find the bathrooms, just come and see me, I kind of stand out in the green top today, and in case of a fire, the same thing. We've got exits there, but you know the drill. So I'm not going to go on about that. More importantly today, we’re here to hear from some experts in the information and privacy fields and as I said it's a pleasure to be here as a guest of the Office of Information Commissioner. And joining me now is newly appointed Queensland’s Information Commissioner. Would you please welcome Joanne Kummrow.

Joanne Kummrow

Good morning, everyone. As Kim said, my name is Joanne Kummrow and I commenced as the Queensland Information Commissioner on the 3rd of April. So I've just clocked up my first month. It’s a pleasure to welcome you to a Privacy Awareness Week 2024. My first PAW event in this new role. On behalf of the OIC, I extend my sincere thanks to Uncle for his warm and generous welcome, for all of us present today, the State Library of Queensland and online. Privacy Awareness Week was established by the Asia Pacific Privacy Authorities or APPA in 2006 and it’s held in May each year. Public and private sector organisations from across the Australia Pacific region host a variety of special events and initiatives during Privacy Awareness Week, to raise community awareness of

information privacy rights and the responsibilities of government sector agencies and at the Commonwealth level, the private sector, when they are collecting, using and storing personal information. The theme for this year's PAW is privacy and technology, improving transparency, accountability and security. There's undoubtably a convenience, and undisputed efficiencies that arise from the use of new technologies in collecting citizen's personal data. As we embrace new digital technologies, it's critical that the public and business sectors do not lose sight of the fundamental human right to personal privacy. And as Uncle spoke of barma, really at the heart of every, everyone is a human being and privacy is a key part of being a human.

In the years following the second world war, the universal declaration of human rights was adopted and proclaimed by the UN general assembly in December 1948. Article 12 provides that no one shall be subjected to arbitrary interference with their privacy, family home or correspondence. And that everyone has the right to the protection of law against such interferences or attacks. In Queensland, closer to home, this privacy right is enshrined in Section 25 of the Human Rights Act, where a person has the right not to have the person's privacy, family home or correspondence unlawfully or arbitrarily interfered with. It's also the basis for the Information Privacy Act which has the primary objective to provide for the fair collection and handling in the public sector environment of personal information. These responsibilities involve agencies and companies ensuring they adopt a privacy by design approach when embarking on embracing new technology projects, and that they have a firm commitment to being transparent around their collection and use of citizen's personal data. This also includes being open about what data has been collected and why, and how it is to be used.

Being accountable for the lawful and proper collection and use of personal data, including only collecting the minimal amount of data required, using it for the purpose for which it's been collected and not keeping it beyond the period for which it is required. Finally, keeping personal data secure. Whether the data is held directly by a government agency or company direct, or company directly or by a third party, at the core of keeping data secure is recognising that information is an asset. As such it is important to know what information your agency holds, for example, by way of an information asset register and how that information is being managed and kept secure. I extend my sincere thanks to our keynote speaker, Australian Privacy Commissioner Carly Kind and our panel of speakers today, who will explore issues around information privacy and improving transparency, accountability and security, as we embrace and adopt new technologies now and into the future. Finally, as you will be aware, in November 2023 the Information Privacy and Other Legislation Amendment Act 2023, was passed by the Queensland Parliament. Amongst other things the Act amends the Queensland Information Privacy Act, including aligning the definition of personal information in the IP Act, with the Commonwealth Privacy Act, adopting a single set of privacy principles, based on the Australian Privacy Principles and the Commonwealth Privacy Act, and will now be called the Queensland Privacy Principles. Establishing a mandatory notification data breach scheme, which will require agencies to report eligible breaches to affected individuals and my office, providing enhanced powers and functions for the Information Commissioner under the Information Privacy Act, including a power to investigate on the Information Commissioners own motion.

As part of the new legislation, the OIC is undertaking a major implementation project around these important reforms. This includes providing guidance and training to Queensland agencies, to inform them about these changes and assist them in ensuring, assist them in ensuring that they're well equipped to meet new obligations under the Information Privacy Act. Our resources will be published in due course over the coming months on a dedicated iPolar reforms webpage that's accessible via the OIC's website at www.oic.qld.gov.au. To access our new resources, training and guidance on changes to the IP Act, please visit our website and also subscribe, consider subscribing

to our weekly newsletter to keep up to date. I hope everyone enjoys Privacy Awareness Week. Thank you, Kim, for your anecdote. It's important, I think we're all very, well privacy informed in this room and online, but I sort of challenge you to go away and speak to someone, like your parent, like a neighbour, who may not be as aware, and just have a quick word to them and ask them about privacy and get that dialogue going, because at the end of the day it's important we're educating agencies, but it's the community that we want to raise awareness with and I think we all have a part to play in that. Thank you so much for your time.

Applause

Kim Skubris:

Well, I shared with you that we are live streaming our launch event across Australia, but I'd now like you to turn your attention to an international scope, where we're joined by UK's Information Commissioner, John Edwards. If you'd like to cast your eyes up to the screen. Thank you.

John Edwards

Good day. I couldn't be further from the golden sands of the Gold Coast and the temperate tropical climate, but I'm having a great time here in the UK. I'm very interested that your (ui) privacy and technology, improving transparency, accountability and security. Three time with some work that we're doing, themes that we're pursuing this year. This year of course, a year in which AI is really going to bed in and transform our lives, it was just like a freight train last year. I and other regulators over here in the UK, have committed to take a head office way of not being swamped by it. There is a sense internationally that we as privacy regulators and policy makers really missed the boat with the business models underlying social media, and even search and ad technology. We're committed not to do the same thing with AI. There's been a lot of quite apocalyptic talk in the last 12 months or so. I don't know if you've noticed, but comments like, you know, this is a regulatory wild west, these dangers are here and present. And I think to a degree some of that is overstated. The UK, with its UK GDPR is, has a technology neutral principles-based approach to regulating for the safe conduct of personal data and personal information, just like Queensland. Your principles of security, access, transparency, use limitation, these are all derived from those 1980 OECD principles. So we have this common, this common genealogy in our approaches to regulating in this area. And those principles give us quite a great, you know, quite a degree of scope to approach new technologies with our existing tools and demonstrate how these tools are able to fit. So when you look at, for example, the things of accountability, transparency and security, these are all requirements of the UK GDPR as of the Queensland Data Protection Law. And when the government in the UK issued a white paper to consult on its regulatory approach last year, it suggested that it might regulate based on principles not dissimilar to those, that there should be transparency, explainability, accuracy, that AI models should avoid unfairness and discriminatory, you know, embedding systemic biases based on the training data sets. Well all of those values are protected and reflected in the UK GDPR. So we've adopted a position at the ICO of demonstrating how they can apply. We tend to work both upstream and downstream, and by that, I mean downstream being something has happened, and we will apply the regulatory tools to it. We did this last year with a number of local authorities who were deploying artificial intelligence solutions to assist their administration of welfare payments and alike. We did it with the Department of Welfare and Pensions and we found that despite the concerns being raised by civil society, the AI deployments were really being used just to get some

administrative efficiencies and were not replacing human intervention with automated decision making and were not perpetuating biases and data sets.

So again, the role of the regulator in that case is to investigate and provide reassurance to the community that we can get the benefits of these technologies in ways that do respect the privacy of the individuals whose data they are using or rolled out across. In commercial applications, we took snap (?) to task. It rolled out a generative AI chatbot as part of its Snapchat platform. And we expressed reservations about the degree to which they had done a fulsome ex-anti risk assessment, which is a requirement for high risk processing over here and I don't think you've got quite the equivalent in Queensland. But it is a mechanism by which I, as the regulator, and my team can hold innovators to account. We may not say this is technology which is lawful or unlawful, but we can say show us your workings, show us that you've investigated, identified risks and put steps in place to mitigate those. So that's our kind of traditional downstream regulation which I'm sure you're very familiar with. On the upstream side, we think it's important that we are able to demonstrate to innovators that there is a legal framework, that it can be applied to the new technologies and that there are not the kinds of regulatory gaps that some commentators have suggested.

So for example, we've issued guidance on AI and explainability, guidance by the way which pre-dated the issuing of ChatGPT by a couple of years. We issued that guidance in conjunction with the Alan Turing Institute. So it's, it's really helpful to have these networks to discuss how these new technologies can be regulated with our existing tools. We have a consultation out at the moment on generative AI and some of the challenges that large language models present in terms of the collection principles. I mean you have your own collection principles which say that, you know, ideally, we could default to collecting directly from the individual, but certain practices of collecting publicly available information are permitted. But again, that happens against the background of data minimisation, proportionality. Here we have a concept of lawful basis, you have to be able to describe a lawful basis for your processing or collection of information. We're looking at the likelihood that legitimate interest will be found to be a lawful basis for the training of foundation models of large datasets. But when you use that legal basis, you're obliged to undertake a balancing test about the public interest, the interest of the individual concerned and the interest of the data controller. So again, it's a mechanism for showing some controls and guardrails for the development of these technologies. I'd welcome your thoughts on our consultation, on generative AI on our website, ico.org.uk, but increasingly we find it's so important to collaborate with other regulators as well. Internationally, as I very much enjoyed with APPA and I know that you will be confronting these issues with your colleagues around the Asia Pacific, but increasingly it's important domestically and you've got a wonderful competition regulator in Australia which is really leading the world, I think, in showing how data protection values can be enforced through competition law.

Here in the United Kingdom we have an organisation called the Digital Regulation Cooperation Forum, and that is bringing together the Financial Conduct Authority, OFCOM, the Communications Regulator and the Competition and Markets Authority, together with the ICO to identify cross-cutting regulatory issues and make statements to the market about how we are going to reconcile what might appear to be conflicting regulatory duties across different regimes. The DRCS has been funded to provide a multi-agency advisory service, a digital hub which will give information to innovators about how the exiting regulatory regime applies to these AI innovations. And that's in addition to our own innovation hub, which we commit to provide advice on new technologies within ten days. It's an addition to our sand box, in which we invite developers to bring their initiatives in and work with our teams to see how they can be done compliant with the law.

So there is plenty happening in this space. It is not a regulatory gap, and I know that Queensland will be the beneficiary of some of the work that we're doing and it's happening elsewhere. Please do help yourself to it. It's important that we get some unanimity of approach to regulation internationally. So introducing what we're doing here in the UK to your Queensland state legislative bodies, I think would be really important and helpful. And I really look forward to hearing how you are meeting the challenges of transparency, security and accountability in this digital age. Thanks again for the invitation to talk to you. I'm really sorry I can't be there in person, but I hope you have a great Privacy Awareness Week.

Applause

Kim Skubris:

Thank you to John Edwards, the UK's Information Commissioner, and as John shared the importance of having a uniform approach, it's quite an interesting time for Australia with legislative overhaul due this year for the Australia Privacy Act and at the helm is Australia's Privacy Commissioner. I'd now love you to join me in giving a warm welcome to a true, well I won't say true blue Queensland, true maroon Queensland at heart, who's come back from London, but is joining us from Sydney today. Did you follow the bouncy ball then? Anyway, please welcome Carly Kind. Thank you very much.

Applause

Carly Kind

Hello everyone, and happy Privacy Christmas, which is what we call Privacy Awareness Week, if you're a real privacy geek. Thank you so much, Kim, and thank you to Joanne Paxton for having me, inviting me to speak today. I'd like to begin my extending my respect to Uncle Billy and to all First Nations people who are here with us today. I found his words really struck a chord, in particular thinking about how we ensure that progress and change work for all people in society, and I think that really connects with the big technological changes we're undergoing at the moment, some of which are really challenging many groups if different ways and how the big challenge we face in how to ensure that that technological revolution delivers benefits for everyone. I'm really honoured to be here today, not only because I'm here as the newly appointed Privacy Commissioner in my first Privacy Awareness Week, but also because I'm here in a city where I first became interested in and passionate about privacy.

I was a first-year law student at UQ when the planes flew into the Twin Towers in New York and so the early years of my study really coincided with the end of, kind of the post-Cold War era, and the beginning of this new phase of the Global War on Terror. And observing this as an interested law and politics student, really shaped how I come, came to understand about state power and abuses of state power and the importance of human rights law, in that context. And it was through that lens that I became interested in the right to privacy and its curtailment by expanding national security protections and growing surveillance powers that we saw in the first few decades of this century. And I was then really fortunate to commence my career as a young lawyer in a small law firm, just across the bridge at 8 Petrie Terrace, which was then Boe Lawyers, under Principal Andrew Boe. And at Boe I worked with really passionate lawyers who showed me how law and policy could advance and impede the enjoyment of social and racial justice. So the combination of these two experiences, my years studying law at UQ and then my experience working as a young lawyer, particularly in the

criminal courts here in Brisbane, really motivated me to want to pursue a career in international human rights law and then later at the intersection of technology and human rights.

Over time I've come to understand that the right to privacy is a key means by which power is mediated, limited and expressed. In the early 2000's when we saw increasing national security intrusions into the personal realm, there was a lot of expanding surveillance powers and anti-democratic measures justified under the banner of counterterrorism. Infringements into privacy were one way in which power was exercised over individual journalists, activists and advocates, and it became clear to me that privacy is a fundamental enabling right, for a range of rights, not only those related to procedural fairness, but also expression, opinion and self-determination, and that at its core it is about power. I forgot to hit the start on the slide, apologies. Motions of power cut in every direction in the digital eco system. The power wielded by tech monopolies and duopolies, the power concealed in political microtargeting and misinformation campaigns, the lack of power and agency consumers feel when they're using digital technologies. Information about us is core to who we are, and it's closely linked to our ability to determine who we are and what we do in life. When we have control of our personal information we are empowered, but equally when others can access and use our information, they are wielding power. It has been evident for a long time that government access to and use of personal information can operate as a means of exercising power and can potentially disempower individuals. Indeed, the early founders and builders of the internet saw that technology as a means of ousting government control and placing it in the hands of individuals. John Perry Barlow, who was one of the founders of the earliest digital rights organisations, the Electronic Frontier Foundation, wrote something called the Declaration of the Independence of Cyberspace, arguing that governments should have no jurisdiction in the online realm at all and that no laws should apply there.

That was in 1996. Only a few short years before the first anti-trust case in the digital realm would establish the harms of online monopolies. It was Microsoft then that was under the scrutiny. And about a decade before smart phones and social media companies would change the paradigm of the internet forever. And since then, we've come to understand more about companies, how companies too can wield and exert power over individuals by collecting, using, selling or tracking their personal information. Seminal moments have occurred in the interim. Of course, the first that comes to mind is the sale of data from a small group of researchers to a political consultancy called Cambridge Analytica, and the use of that data to influence the US presidential election. Another one that comes to mind is the case of a teenage girl who began receiving promotional material for baby related products from Target before her parents knew she was pregnant. These moments began to bring home for individuals just how much power organisations that hold and use personal information really possess. In Australia the major data breaches at Optus and Medibank in recent years were similarly seminal. They exposed to Australians, not just how much personal information these companies collect and hold, but what the real consequences of losing or compromising that data are. A tragic reality faced by the owners of more than 100,000 Australian passports that were compromised in those breaches. The result is that today we see increasingly high levels of interest in, and value placed on personal and data privacy.

This hasn't always been the case, of course. Throughout history the community's privacy attitudes have been cyclical. In 1999 the CEO of a tech company, Sun Microsystems, said that consumer privacy issues are a red herring, you have zero privacy anyway, said Scott McNealy, get over it. In the same year Pew Research shows that only 16, 1% of online users, were worried about privacy. In a, quite a quaint comparison their research, so this is from 1999, captured 29% of users who don't go online at all, who were worried about privacy. Only 20% of internet users worried that their email

might be read by someone other than the party they sent it to, and 42% said they did not worry about that at all. This was a really fun dataset to dig into, by the way, it included this gem, 41% of internet users were worried about the threat of computer failures related to the Y2K.

So if we compare that today, that data to today, so 16% of people worried about their privacy online. If we compare that today, a study also by Pew Research shows just how much higher levels of privacy, literacy and privacy concerns are. For example, most people, about 75%, believe they have little or no control over what companies or government do with their data. That's in the US. And we've seen an increasing concern about and value for privacy here in Australia too. In our own research conducted by the Office of the Australian Information Commissioner last year, of Australian attitudes to privacy, for example, the proportion of Australian adults were care about, enough about privacy to do something about it, increased from 75% to 82% over three years. Our research also showed us that nine in ten Australians have a clear understanding of why they should protect their personal information. Only two in five people feel most organisations they deal with are transparent about how they handle their information and 58% say they don't understand how it's used. 84% want more control and choice over the collection of their information. And there was a common view that businesses and government agencies should do more to protect Australian's personal information. 89% would like government to pass more legislation that protects their personal information. This trend towards valuing privacy more and more is reflected around the world. If we look at, just at trends in regulation, from 21 to 23, 17 countries enacted new data privacy laws, bringing the total to 162 globally.

And there's even now draft privacy legislation under contemplation in the United States, which is the jurisdiction historically adverse to privacy legislation at the federal level and it seems possible that that country will enact a privacy law before the end of the year. So it's against this back drop then that we celebrate Privacy Awareness Week, at a time in which awareness of privacy is actually higher than ever before. Expectations for better privacy practices are stronger than ever before. Recognition by business of the ethical imperative to be good privacy players is more widespread than ever before, and yet privacy harms are still everywhere. Data breaches occur weekly. Data driven business models are still pervasive and individuals still feel a lack of agency and control when it comes to their personal data. For that, for that reason this year we're calling on people, organisations and governments to power up privacy, to take control and to step things up. We really want to see entities inject some power into their approach to privacy, rather than simply being in responsive mode or dealing with privacy issues late in the day. We would like to also see government power up privacy Australia-wide, by introducing reforms to the Privacy Act that are so overdue.

In doing so, we believe we can restore some power to individuals to feel in control of their personal information once more. Short side bar for those of you who aren't aware, the IP Act that Jo was talking about before, governs the use of personal information by public sector agencies here in Queensland, whereas the Commonwealth Privacy Act that I oversee, governs the use of personal information by Commonwealth, agencies, as well as other organisations in the community, including businesses. So now is a, especially ideal time for businesses and government agencies covered by both Acts to power up existing privacy practices and cultures in advance of privacy law reform. Early last year the Attorney General's department completed its review of the Commonwealth Privacy Act and the Australian government responded in September agreeing or agreeing in principle to everyone, except ten of the 116 proposals for reform. And thankfully the Federal Attorney General announced last week that at the request of the Prime Minister he will bring forward legislation in August to overhaul the Privacy Act. There are many elements to the reforms, but taken together

they will power up privacy protections by answering a need in the community for the proper protection of their information and increasing private and public sector organisations accountability for their privacy practices. Really key to the privacy reforms is the introduction of a new standard, which is that all personal information handling must be fair and reasonable. This is a fundamental shift in approach that will require organisations to ensure their practices are fair and reasonable in the first place, not being able to lean back on consent as some kind of shield, but rather ensuring that fairness and reasonableness are key.

The reforms will also provide a greater range of powers to the OAIC, my office, reflecting the Australian communities growing expectation that its regulators take more enforcement focused approach. Other important developments include enabling individuals to exercise new privacy rights and take direct action in the courts if their privacy is breached. These initiatives reflect the baseline privacy rights expected by our community. One key proposal relevant to our discussions today, around privacy and technology, is a new requirement that has been agreed in principle for organisations to conduct a privacy impact assessment for activities with high privacy risks, which is already a requirement for Australian government agencies. Queensland too is powering up privacy protections afforded to Queenslanders by your public sector agencies. The reforms introduced by Polar increase consistency and privacy rights and obligations across the Queensland and Commonwealth jurisdictions. Alignment between the frameworks is really important for regulators, for regulated entities and for the individuals we look to empower. Harmonisation increases, sorry, decreases compliance costs for regulated entities and provides clarity and simplicity and importantly for individuals it helps ensure their data is protected wherever it flows. Privacy law reform offers real opportunities for Australia. There are substantial gains to be made for the Australian community through the proposed reforms, particularly those which address gaps in protections for children and vulnerable groups.

There's clear community concern around data breaches due to the events of recent years and the reforms of the breach notification regime, as well as stronger enforcement powers available to us as the regulator, will enable much more decisive action to be taken with respect to data breaches. There's also excitingly the potential for the Australian regime to leapfrog equivalent frameworks oversees and take some novel approaches, such as the fair and reasonable test. And this allows us to learn from the experience of other regulators in recent years, particularly as they've grappled with new technologies. I come into this role having spent the last five years on AI and data governance policy, as Director of the London Base Research Institute, the Ada Lovelace Institute. We had a role to remit to ensure that data and AI work for people and society. In that role I thought a lot about the role of data privacy regulation and regulators in grappling with new and emerging technologies, particularly AI.

I know that this is probably the biggest issue on many of your minds at the moment, how is AI going to change our societies and how will important societal values, such as privacy be protected in a world in which AI is ever more pervasive. Many of these technologies are incredibly powerful and some of them centralise power in new ways. For example, generative AI tools are disrupting industries where power has been historically centralised. But they can also be a means for powerful entities to amass power, including market power. The OIC is working hard to understand the implications of AI for privacy, including with our colleagues in other regulators, through an initiative called the Digital Platform Regulators Forum, which was inspired by the organisation that John was talking about in the UK, which is Analogist. And here in Australia ours is made up of the OAIC, the ACCC, the ACMA, the communications regulator here, and the eSafety Commissioner. And we're working together to understand the implications of AI. We've published working papers on

algorithms and LLMs, as well as other issues. At the OAIC online privacy and higher privacy impact technologies, including practices involving the use of generative AI, face recognition and the use of biometric information, are high on our list of regulatory priorities. We have made determinations concerning the collection of biometric information by Clearview AI and 7-Eleven to match facial biometric templates and we have ongoing investigations into the use of facial recognition technology by Bunnings and Kmart. These technologies typically rely on artificial intelligence through the use of machine learning algorithms to match templates. And they constitute some of the most concerning technological developments from the perspective of the Australian community. We've also begun scoping what other new and emerging technologies might create privacy risks and harms that warrant our intervention.

We've opened preliminary enquiries into the use of personal information in connected cars, for example, and the sharing of personal information between car manufacturers and other entities such as insurance companies. We're also looking closely at and taking enforcement action around practices that impact individuals' choice and control, such as opaque information in terms of service, technologies and business practices that record, monitor, track and enable surveillance and practices that involve the use of generative AI, facial recognition and the use of other biometric information. Finally, I think it's incumbent on regulators also to think about how new technologies should inform our regulatory practice, either through necessitating new investigative techniques, such as algorithmic audits or through deployment inhouse of AI technologies to streamline complaints handling and provide more efficient access for, information access to the citizens and so we've begun looking at this at the OAIC. Although many of these technologies are still on the horizon, I encourage all organisations, especially when considering new technologies, to put some practices into action now. Privacy by design across the information lifecycle, privacy impact assessments and asking the community whether, what the, whether the community consider what you're doing to be fair and reasonable, importantly that is the standard that we hope will be legislated later this year. These all go to accountability. There's a good reason to do them and to show privacy leadership, because getting privacy right provides social licence for new initiatives. Organisations and agencies that get it wrong, face real consequences in terms of the community's trust and confidence.

Data breaches are an area where many Australians recently have had a tangible experience of privacy issues and the sense of disempowerment they can bring. Since the Commonwealth Notifiable Data Breaches Scheme began in 2018, the OAIC has been notified of 5,800 data breaches, in six years. Our community privacy attitudes research found that almost one in two people surveyed had experienced a data breach and three quarters had experienced harm as a result. It also told us that Australians consider data breaches the single biggest privacy risk they face. There are high levels of public concern about data security as a result of these breaches and a strong appetite in the community for organisations and agencies to be held accountable. Mandatory reporting of breaches strengthens the protections afforded to everyone's personal information and improves accountability and transparency in the way organisations respond to serious data breaches. So the introduction of mandatory reporting in Queensland is a really important opportunity to build public confidence and trust in government's handling of personal information and empower individuals to take action to manage risk and mitigate harms should a data breach occur. It's really important for us to think here about security and cyber security. About 40% of the data breaches notified to the OAIC have been the result of cyber security incidents.

So it's incredibly essential that organisations put in place measures that guard against threats. Recently we're seeing the downsides of the increasingly interconnected economy and data breaches that involve multiple entities. Kim mentioned the New South Wales Club's breach from last week

and that is an example where a third-party supplier was the cause of the breach, and this is increasingly common. So we really need to see organisations step up how they ensure the protection and privacy through contractual clauses as well. The response to a data breach matters. Australians have shown to be quite forgiving, and they are more willing to invest in a company, if they see a company is responding quickly to a data breach. But where noncompliance is persistent, our office will take action. We have recently commenced our first civil penalty proceedings in the Federal Court against Australian Clinical Labs, resulting from an investigation into its privacy practices that arose from a data breach in February 2022. That case took eleven months to reach the Federal Court and so it should serve as a warning for businesses to lift your gain or risk enforcement action.

I know I won't be the only one in the room who reads the news every day and sees privacy as central to so many of the issues that challenge politicians, policy makers and ordinary people. There are the repeated data breaches, of course. Just last week there was New South Wales Clubs, as well as the incident with the Qantas app. There's also the continued concentration of immense power in the hands of a few large tech companies, which causes problematic dynamics in digital markets. As evidenced most recently by the reticence of one tech boss, who shall not be named, to comply with regulatory restrictions in the safety realm. There's also the seemingly unstoppable growth of AI, and in turn the continued concentration of power in those same few companies who control much of the infrastructure, compute and data, likely to fuel the AI revolution.

There's even the continued scourge of misogyny online, as recently identified as one of the key components of persistent egregious levels of domestic violence in this country, which is impart fuelled by the incentives of the online attention economy. All of these issues and many more relate to privacy and in my view could be tempered or mitigated through stronger, better privacy protections. Which is not to say that privacy alone is the solution, but that at the very least privacy maybe the starting point. Now this is unsurprisingly the view of someone who works in privacy and believes whole heartedly in the right to privacy and in privacy regulation. When you're a hammer, everything looks like a nail, but if the dinner tables I'm at are anything to judge by, it is also instinctively the view of many of our fellow citizens and consumers.

Privacy is on everyone's lips these days. So as we stand at the precipice of a new era of technology and markets, we are urging Australian businesses, agencies and other organisations to meet this challenge, to power up privacy and make a real difference to the community. Powered up privacy practices are good for everyone, for consumers who feel more confident participating in the digital economy, for businesses which could boldly innovate knowing that guardrails are in place to protect customers and for government which can realise the benefits of new technologies with the trust of its citizens. Thank you very much.

Applause

Kim Skubris

Carly, I'm sure I can speak on behalf of everyone here and online around Australia, we're very happy for you to be the hammer and nail at home, and you've brought up some fascinating insights there which I'm really looking forward to discussing with you now. I would now like you to join me in welcoming to the stage our panellists for today, Scott McDougall is Queensland's Human Rights Commissioner. Please make Scott feel welcome.

Applause

Kim Skubris

Along with Chris McClaren. Welcome, Scott. Chris McLaren, Chief Customer and Digital Officer, Queensland Government Customer and Digital Group. Thank you, Chris.

Applause

Kim Skubris:

And Paxton Booth, Privacy Commissioner for Queensland. Thank you very much for joining us.

Applause

Kim Skubris:

Invite you to adjust your microphones so everyone can hear you okay. Carly, I'm going to start, I can't help myself, as a journo, I'm just going to say straight out of your share there, I'd like to start by asking you, you mentioned that the new legislation would put the barometer of fair and reasonable and you shared your office is currently prosecuting an organisation. Do you feel that the overhaul of legislation that's coming in August will be enough to give you the power to really hold organisations and individuals accountable. Is it going to be enough and is it enough for you that the laws will be toughed?

Carly Kind:

A good thing about the Privacy Act reforms having taken almost ten years to get to this stage, is that they really have, there really has been a very rigorous process of review that's involved many experts. Our office has contributed a lot as a stakeholder to that review. So it is a very impressive bundle of amendments that span right from addressing what organisations can do when they're handling data in the first place, the particular groups that require particular protections. So it includes for example the power from my office to develop an online children's privacy code, and then it also speaks to the enforcement powers. So you're right to identify the limited enforcement powers that we've had to date, which means for example we've only been able to take entities to court where we can establish that privacy violations are serious and repeated, which is quite a high standard. Newer lower levels of penalties are hopefully going to be introduced to the reform. So from our perspective it doesn't cover everything we would have liked, but it's near enough there that it covers the entire kind of spectrum of the Act and we feel is just what we need to take, kind of privacy protection into the new era.

Kim Skubris:

Thanks, Carly. Chris, from a Queensland lens, we've heard from Carly, obviously from a Commonwealth lens. Can you explain a little bit about your agency and what your role is...

Chris McLaren:

Sure.

Kim Skubris:

...and how you're balancing obviously getting an increasingly digital platform for the Queensland Government, but also considering all of the issues that Carly shared in her keynote.

Carly Kind:

Yep. Great, thanks, Kim. Yeah. So in my role as Queensland Government Chief Customer and Digital Officer, I cover privacy, privacy related topics from a couple of dimensions. First, you know, is on our cyber security unit, we obviously have an active role in helping agencies, statutory bodies, have the right measures in place to protect information that they might be holding. We have the open data team or a data and AI team and one of our obligations there is to provide a level of transparency to the business of government and comply with an open data policy to give that level of transparency and obviously there's a trade-off between transparency and privacy. And then we're leading our work around digital identity, which is intended to make it easier for Queenslanders to engage with government and other services with more control over their personally identifiable information. And then the, probably the fourth component is really building out the set of platforms that, you know, I describe it as a piece of shared digital infrastructure that allow agencies to plug into that infrastructure to make it easier for them to engage with citizens and businesses with the right level of security, privacy, design, accessibility built in, to take away the burden of, yeah, of that from individual agencies.

So we can all operate at the maximum level of security, privacy, compliance and safety. We also have carriage of a lot of the policies that we dictate across Queensland Government. Ensure that agencies are doing things like privacy impact assessment, they're following, you know, we give them some, a variety of tools for when they're publishing data to the open portal, to ensure that they're able to do the right sorts of risk assessment checks and privacy checks. We're actually going through a process at the moment of doing a complete review of the open data policy to ensure that it's still fit for purpose. You know, with the emergence of new technologies it's, you know, we always have to be worrying about things like reidentification risk and things like that. But, look, just, you know, from my stand point I think there's definitely, I think in this country there's a, we've become complacent about privacy. I, personally I'm a, I would describe myself as a privacy maxi, and I think everybody should be a privacy maxi. I think we've got to a point somewhat in society where if you're asking for privacy, that almost implies that you're up to no good or you're doing something wrong. Privacy is absolutely a human right. It is the right for an individual to reveal themselves to the world in a way that, that they see fit to who and when and how, and I think somehow, we've lost that and we've just gradually let our, our privacy get eroded over, over time. And I'm not surprised to hear some of those statistics that you raised in the UK. We should all be defenders of privacy. I heard someone say one time that look, Chris, I don't care about privacy because I've got nothing to hide, and I just think that's a flawed argument. It's a little bit like saying I don't care about freedom of speech because I've got nothing to say. We all absolutely need to care about privacy.

Kim Skubris:

Thank you, Chris. Paxton, you're nodding away here. How do Queenslanders, do you think rate, compared to the rest of the country when it comes to their attitude to privacy, as our Privacy Commissioner, and as secondly, when we're considering legislation, how do we fair, compared to other states? Are we doing enough here to protect people's privacy from a legislative point of view?

Paxton Booth:

I think I'll start with the second part first. We're certainly making some progress in terms of our legislation and making some advances, getting up to speed around the protections that Queenslanders are entitled to, around making sure that government agencies manage our personal information in appropriate manner, and as Carly mentioned, presentation, that the mandatory notification of data breach regime is an important step forward for Queensland and we'll be the second state in Australia to introduce that, New South Wales being the first state. To see that come to fruition is going to be really exciting for us. I think it's one way which government agencies manage trust, communities and people in the community to make sure if there is a data breach and something happens, people are told. They'll quickly, not only told about the breach, but actually given some instruction about what they need to do. I think one of the things that people can get a sense of when they're told of a data breach is sense of overwhelm, what should I do, how do I respond to this.

So by giving people more information to empower them, to take action to protect their identity is really important step in the mandatory breach notification scheme, it's not just the box, help people move on your way, it's about making sure they understand what they need to do to protect themselves (ui) breach. In terms of Queenslanders overall in their, I suppose, their sense of acquiring privacy rights, I think we're, I think we're pretty good across the state. A lot of the complaints we get coming into the office about breaches of privacy, it's really clear that a lot of people are really in tune with their rights and understand a lot of the privacy principles in the Act, which is really encouraging to see. And I think we've seen over time, as Carly pointed out, a real increase in people's, both capacity to understand the potential risks in privacy, and also their expectations on business and government to manage it appropriately. Whether it starts with, whether it starts with the collection of their information, not handing it over unless you need to, and also expecting the companies are managing it and moving their information where they no longer need it and putting in place the right kinds of protection, to make sure (ui).

Kim Skubris:

It's an interesting point and I'm just thinking, I'm sitting here thinking about my 16-year-old, going on 30, he'd be more likely to say, hey, no, I'm not handing that over, his generation. My parents in their 70's, even myself, I'll share, I was sharing with Joanne earlier, this time last week I jumped in an electric car in Townsville to go to work. I have my own communications consultancy now, and I jumped in the car and let's call him Bob Smith, I turned on the engine, which I wasn't even sure if it was on yet, it was so quiet, but suddenly everything flashed up on the dashboard, and it actually was quite confronting. It was obvious the person who was in the car before me, as I said, I'm not going to say his name, it was unusual, like Skubris, which also threw a few red flags for me, and his name came up, and I am not by any means technical, I go to my boys to help me out, but even for me, with

my lay approach to it, I was able to play around with the dash, I was looking at Apple CarPlay, I could see what he was playing on his, you know, what he, what music he was playing and I actually, I know there's the long arm of the law here, you can share with me later, I had to make a phone call during my trip. I had my phone on speaker, and I thought I have to pull over, because otherwise I'll be pulled over, I did not want to attach my phone to the car and the computer.

And I notice, Carly, you had one of those headlines up there, modern cars and, so to the point we're talking here now about agencies and what we're doing, but what about, Privacy Awareness Week is about all of us. It's about awareness, about consumer awareness. I'd like to throw this over to all the panel from human rights lens, Scott, and to Carly, with your background in human rights. But what can we as consumers do, what are the key things we can do on top of education to really, do we push back, like I just did or I felt a little paranoid, like Big Brother was watching me, but I did not want to put my phone attached to the car. I didn't want Kim Skubris, the next person to jump in and see my name. Is that fair or am I being paranoid? Scott?

Scott McDougall:

I think it's fair enough, and happy Privacy Awareness Week, everybody. I, look, I had an experience recently at the Yamba Bowls Club, so in New South Wales, where, you know, the kids are hungry, you're trying to get dinner, but to just to enter the club you've got to handover your driver's licence, and they put it through a machine and God knows where that information goes. So, and in that position often consumers, you know, are not in a, a strong bargaining position to negotiate their privacy rights. But I do think there is consumer power. The more people who do make a point, even if you said look, I understand this, you're just following your rules, but please tell your boss that I'm not happy about handing over this, this card. Little things like that might help. But it is, it's so pervasive, the invasion of our privacy on a daily basis. And one of the things I was going to talk about is the human rights framework as a means of responding to privacy issues. And I think that it's interesting to hear Carly talk about her unreasonable test. In the Queensland, the Human Rights Act, we do have a proportionality test. I want to encourage all the public servants here to go and read Section 13, just to remind themselves. But the real value of that test is it forces decision makers. So those people who were designing new technology, to look at the alternatives to what they're doing, to see whether they can achieve their legitimate and purpose, in a way that is less restrictive on the rights to privacy of the end users. So that's a really valuable tool in my view. I think it does, not quite marry up completely with fair and reasonable, but they are fairly closely aligned, and I think Carly mentioned good points about the value in trying to line up state and federal laws as much as possible to get that consistency of message across. And just going back to your original point, in terms of people being in a position to advocate for their rights, the simpler the test is for your everyday citizen to understand it, so fair and reasonable, I think the more likely they are to take up their case.

Kim Skubris:

I was thinking what John shared in the video about it, not just being uniform, well he was sharing, you know, across the globe, that if, you know, I'm thinking about travelling and being in an airport and the facial recognition or whatever it might be, that if it's uniform across the globe, people have more chance of making a case and applying it. Carly, through, as you said, your background with human rights, looking through that lens, would you agree with what Scott's sharing there?

Carly Kind:

Absolutely. I think that, I mean, not to get down in the wonky details of legal standards, but I think the proportionality, or in Europe it's called necessary and proportion is the standard. We hope it will very much marry up with fair and reasonable. And actually, the US, the draft US legislation which just got published last week includes necessary and proportion as a standard too. So as Scott alluded to, that standard basically means, you know, think about in all the circumstances. Yes, this might be helpful, but is it really, do you really need it and couldn't you use less intrusive means to achieve the same objective. I think that's really about pushing organisations to think, you know, what is the, like flow on effects of what you're doing. Facial recognition is a great example. Putting aside whether or not the technology works as it says it does, and I think there's some real question marks there. If that technology works perfectly, it may be very helpful to some organisation, for example a supermarket that wants to reduce, wants to be able to go after shoplifters. It might be a very helpful technology. Is it, are there less intrusive means of achieving that same end, could you have a security guard who's on duty around the clock for example. Would that perhaps be a less intrusive means of going after that same objective and also is the objective itself, how important is the objective itself, for example. Facial recognition isn't going to stop people from stealing things, but it might help you go after the offenders and, you know, really thinking about how important is that objective to my organisation. So I think the standard, whether it be fair and reasonable, necessary and proportionate, is about importing onto those who are collecting and using data, this ethical responsibility to think about, in all the circumstances, what is happening here to individual's privacy and is it worth it for the objective I'm trying to pursue.

Kim Skubris:

It's interesting you say, I'm thinking as a journalist, ethically whether some of my colleagues do it or not, I'm the first to say straight, but ethically we are bound to actually share that we are recording someone or whether it's broadcast, it's on camera or whether it's on your phone, just, you know, their voice. As I said I'm the first to say, some don't. But if that is a litmus test in journalism, dare I say walking into Kmart and not knowing if someone's recording me, I feel like, is simple as having signs up saying you are coming in here of your own recourse, but you will be recorded, but just so we know. And educating to my point of education, because we don't know what we don't know. Chris, how are you finding balancing the challenges of privacy, but also extending, you know, the digital platform? And I guess we're looking through the Queensland Government eyes with you, but I'm happy for you to talk more broadly as well with your experience.

Chris McLaren:

Yeah, actually, I'd like to just call on Scott...

Kim Skubris:

Yeah, of course.

Chris McLaren:

...and Carly. I think, if you look at, you know, like when the Optus incident happened everybody said that's a cyber security incident and I actually look at that and say well that's actually a data collection incident. Why does Optus need to have millions of customers' driver's licence, dates of birth, et cetera, et cetera. Well, they don't. In many situations you'll go up stream and you'll find that there's a law that says they have to collect that, and I think we need to be completely having a fresh look at what laws we've put in place that almost make it so that businesses have to collect information, that really when you think about it, it's not fundamental to that business's ability to operate. So I would draw a distinction between say Optus or the Club collecting driver's licences and storing that information, perhaps say to an IVF Clinic that clearly needs to, you know, invade your privacy with permission to get to a point where they can operate as a business. So I think we need to kind of separate those two pieces and I just, I think this is a key part that we need to solve and there was just something that happened today in the press and I won't name who it involved, but it's out there. So one Federal Government agency reached into a private sector business industry and said give us all of your citizen information, names, dates of birth, addresses and all activity that they've done. And that industry had to comply. And then we wonder why people are losing trust in government. And were those individuals get the opportunity to opt out or were they asked whether or not that information could be shared, no they weren't. And I just, I think that's, that's when we start to get on that slippery slope of really invading people's privacy and I think that's just something we've got to be incredibly cautious of.

Kim Skubris:

So how, what considerations do you look at when you're thinking about introducing new technology and increasing the digital platform? What sort of litmus test do you go through in your division?

Chris McLaren:

Yeah. So everything we do has to have a privacy impact assessment and that's a condition of proceeding through our gated approval processes. As I said before, we are endeavouring to enable government, you know, with 25 agencies and God knows how many statutory bodies, to leverage the best of the best technology. So one of the platforms that we're building is intended to ensure that agencies can leverage what we would consider to be best in class privacy, security, identity, practices and protocols. So every agency doesn't need to be the best, the expert. So one example will be, you know, we've got new data sharing policies that we're building at the moment, but probably the most tangible example I can give is that when a citizen presents themselves and says, you know, there's always a trade-off, right. If you want something from the government, every taxpayer would expect, okay, are you really dealing with Scott, does Scott really need this assistance, you know, we don't just want you to give money to someone who's claiming a benefit without actually knowing who they are. So we've got an obligation to identify who they are. But in doing so we do that in a way where we collect the minimum necessary information through a secure approach to determine eligibility and nothing more. And then if we need to collect, you know, it's agency A and agency B and agency C, we don't ever stitch information together so that we're not, we don't want to create any additional honey pots. So if every, you know, if I deal with Housing and Communities and, you know, different agencies, when Scott say presents to us, we're not creating additional honey pots that

would create a bounty for potential hackers. So we're very mindful of not doing that and allowing citizens to give consent and opting to what information we can share and access between agencies.

Scott McDougall:

Kim, can I...

Kim Skubris:

Yes.

Scott McDougall:

I think it was Mark Dreyfus there, attorney, Federal Attorney General who said we need to shift from seeing that data and especially the unnecessary data that agencies hold, from being an asset to actually being a risk. So I think that is the mindset that needs to change. So necessary data, yes, and have all the protections built around it. Unnecessary information has to have alarm bells going off around it, because it is a risk.

Kim Skubris:

It's interesting you share that, Scott. Through a communications lens where I come from and of course without sharing confidentiality of who I'm talking about, but it's remarkable. It used to be these are almost like, this is our data, we don't want our competitors to find out about it, we're not going to build a common strategy around this because of the, they call, as you said, Chris, the cyber breaches, well really, it's actually data as the collection issue. That they're actually now calling on communications advisors, say what are we do with this, and what if we do have a breach, how, we're going to be proactive with the media. Whereas we used to go, and they'd be kicking and screaming, dragged, to say, admit that they had a data breach. So I think there is a transparency coming from that particular area, which is heartening to see. But it still has the issue and I'd like to ask you all, is that when people, like just the average consumer, feels that they are being violated, you mentioned, okay, what do they do? As our Privacy Commissioner, Paxton, what would you recommend? Because we've got people from around Australia, but what would be the first thing they could do? Contact your office or...

Paxton Booth:

Yeah, look, certainly I think the first thing that people need to understand is the impact on their identity and what data has been released about them. So that will direct what steps they need to take next. So for example if it's their identity information and it's their driver's licence details, there are now an ability to get a new driver's licence issued or a new card number. If it's their financial information, there is capacity to contact your bank and put restrictions, limitations on your banking details to stop people taking out loans in your name. There's a whole bunch of, I suppose, steps you can take depending on the type of information that's been compromised. And this is where I think the agencies have a responsibility to communicate with individuals around what's been comprised and what steps they need to do to minimise the risk. So really reducing the friction for the person

who's been subject to the breach to actually take steps to protect themselves. So point them in the right direction of what agency they need to speak to, and then what they need to do next.

Kim Skubris:

This is not being facetious and again I'm going to open this up, I might start with Carly here. You shared earlier about the security guard. Why don't we have the security guard, instead of facial recognition, say to combat shoplifting. Or we're talking, Scott, you mentioned all this unnecessary, well we were all are talking of this, unnecessary data. And this is a real crossroads here, but is it realistic? We come back to commercially viable, in a world where we're increasingly introducing AI and we're seeing every week in the headlines, these are the industries that are going to be automated. We're not hiring more people because they cost money and they need sick leave and they need, we're going more automated. Is this realistic, how are we going to stop people or organisations collecting unnecessary data? Can I start with you, Carly?

Carly Kind:

Yeah, big question. I'd separate out what you've asked to a couple of bits, Kim. I think first and foremost, this sense of urgency, like we've got to do this now and AI is coming and some of that is a bit overinflated, in terms of how fast technological change is happening. I think we all have a sense that AI is here, and our jobs are going to get taken from us and everything is going to be run by chatbots, but, you know, a big part of that is what we see in the media. The reality, and Chris will be able to speak to this, the reality of technological transformation within organisations and industries is, it's so complicated to do digital transformation, to really integrate these tools into your workforce. It takes some time. So I think not feeding the kind of urgency and fear that makes people feel that they have no control and they have no agency over this thing that's happening without us, at the end of the day technology is within our control. We can make societal decisions about how technology is rolled out in a way that benefits us. We're not at the whims of technology and I think that's really important for people to remember. The second point is to say that technology itself can be privacy preserving.

So thinking about privacy by design, in the design and deployment of technology, means that we can bake privacy in from the start. So more automation doesn't have to mean less privacy protections. Even when you think about some of the really emerging AI applications, there are different ways of doing generative AI, there are things called home amorphic encryption, differentiation privacy. Technical mathematical methods that can be injected into these systems to minimise the amount of personal data they're using and protect individuals on the other end. And there's, you know, pockets, devices you hold in your pockets, like iPhones actually have some of those privacy protections already operating on your device. So technology is not only part of the problem, technology can be part of the solution as well. But there's a big role incumbent on people like us, regulators, policy makers, politicians, to not be swayed by that hype and that urgency and that feeling that everything is out of control. I think really reminding ourselves that law still applies in the online domain, law still applies to technology. We can bring these technologies in our control and direct them at societal benefit, is really key.

Kim Skubris:

Scott?

Scott McDougall:

I am very reassured to hear that from Carly, because I have to admit I do swing to apocalyptic outcomes quite regularly. If anyone saw Australian Story last night, I don't know if anyone in the audience saw that about AI and the impact on the modelling industry. It is really confronting, but I do, and listening to, was it John or you, Carly, talked about algorithm audits? I think if the regulators work together and have enough teeth, I do think there is the capacity to even use AI on itself to help regulate it. So I'm ultimately optimistic which everyone needs to be, but I do think regulators really need a sophisticated approach and they do need to be given strengthened powers. So we do need to be working downstream and upstream and I'll just give my own antidiscrimination act reforms a plug here. So we're hoping that they will be passed in this term of government and they would create a positive duty on all duty holders to take steps, positive steps to eliminate discrimination. And so that would include in the design of algorithms. So that would give my commission a role moving to upstream, rather than just downstream, dealing with all the complaints that come in. And I think that's where we can really see some effective regulatory work in prevention, when you do have that, those functions and powers. So I think we all should have cause for concern, but we should not think that we're heading to the Armageddon.

Kim Skubris:

Oh, the, my boys would say, oh, mum, ChatGPT, you're stuffed as a speech writing. I said, well, actually because it draws everything from everywhere in the internet, I don't think you can surpass the fact you need human interaction. But, yeah, this is the generation coming up and the concern that everything is going to go through ChatGPT, with uni assignments and speeches and so forth. Paxton, when we consider as Carly said though, that let's not place all the doom and gloom, okay, we can use technology though to protect our privacy. Would you like to expand on that?

Paxton Booth:

Yeah, absolutely. Look, for me, I think I see technology as neutral, it not being good or bad, it's about what you do with it and how you use it. So technology has, makes our cars safer to drive, it increases the efficacy, the efficiency and speed with which some medical images are diagnosed. So there's a lot of things that technology is doing that's really good for us. It also can be used up, to up our, I suppose, privacy protections, by use of password managers. There are other software out there which can help reduce the ability for some apps to track our online activities. So there is, I suppose, pros and cons in all of it and it's really about how we decide to apply the technology, what the business decides to do with it. And as we were saying, if you take a privacy by design approach to the use of technology, it can really be advantageous, for not only the business, but for the community as a whole. So I don't, I'm not the kind of person who advocates against privacy, so advocates against technology, but more embrace it with a, I suppose, a set of goggles that enhances privacy when you're doing it.

Kim Skubris:

And Chris suggested earlier, you know, this checklist, for lay terms, how important obviously is that for organisations and individuals when they're going through a new process?

Paxton Booth:

Critical and I think what Chris spoke about was doing the privacy impact assessment and we're really pushing that out. Every time I talk to an agency, I'm, you know, asking did you do a privacy impact assessment on this and more and more I'm hearing yes, which is really encouraging.

Kim Skubris:

What does it actually, excuse my ignorance, can you just run through for some of us who've never done one or faced one, what does it actually entail? What are you getting people to consider?

Paxton Booth:

What we're asking people to consider is, I suppose, throughout the life of the project, how are you collecting, using and storing people's personal information. So as we said, it starts right at the beginning when you're first starting to plan, what are you collecting, do you really need to collect that information to offer that service to the individual. So thinking about, one, the collection, two, how are you going to use it once you've collected it, and is it transparent to the people who you're collecting it from, about what it's going to be used for, and then, I suppose, the last thing is, if you do need to keep it and store it, have you got adequate protections in place to make sure that it's not going to be compromised. We still, you know, there are still (ui) physical data, physical files. So making sure, particularly if it involves physical files, that they're subject to the right protections as well. For example...

Kim Skubris:

Are you talking about filing cabinets?

Paxton Booth:

Yeah, remember those old things?

Kim Skubris:

Yes.

Paxton Booth:

There are still some of us who go in and talk to departments...

Kim Skubris:

I'm old, I get it, yeah

Paxton Booth:

...and actually pull out a file. But we still do engage with people face to face. So it's important, for example, if you're designing a new office space and you're a business who engages with people, are you talking with that person in an environment where you can protect their privacy or are you in like cubicles where you're side by side and I've got to talk to, for example, a medical practitioner or someone and I'm talking about my personal information. Is the person that's waiting in the queue next to me listening to what I'm saying, or have you sort of provided that facility in a space or environment that is conscious of my privacy.

Kim Skubris:

I'm not sure who is better to answer this question, Carly or you, Paxton, but to Chris's point earlier that we need to actually look at leg-, we talked about Privacy Act legislation, but we need to look at legislation that actually deters organisations from collecting unnecessary information. A) where does that lie? Does that lie under, again excuse my ignorance, under the Privacy Act; and B) who is in the position to make, is it federal or state to make these law changes so organisations don't feel obliged or just don't collect unnecessary information from us. You want to vote who...

Paxton Booth:

I think it's both, but I might let Carly go, because I know there's been some big changes in the federal laws around what the federal agencies can do about enforcing those sorts of laws.

Carly Kind:

Yeah. So I think there's kind of two sides to what Chris was saying. I think on the one hand Chris was referring to laws, in addition to privacy laws, that require organisations to keep data for a certain length of time. So for example, telecommunications companies have to retain telecommunications data for a certain period of time. Other law enforcement related legislation requires some organisations to have identity details on hand. In the case of the New South Wales Club's breach, there is New South Wales legislation which says every club, RSL, surf club, has to collect the name and address of every person who enters the door. Now on the face of the legislation it doesn't say keep a copy of the driver's licence, for example, and it says you have to keep it for three years, but not for seven or ten. So there's some gap there between what the minimum requirements are, what organisers, organisations are doing, perhaps over-complying with some of that legislation to retain.

Kim Skubris:

But why, why are they having to retain our addresses?

Carly Kind:

It's very complicated. Some of it is about the protection of, and pursuit of criminal activity. So in the case of telecommunications data for example, it may be in relation to pursuing law enforcement ends. In the case of the clubs, it's most likely, and I'm speaking outside my remit here, to do with compliance with gambling related regulation for example or enabling the, to give effect to exclusion lists. So there's a lot of complicating overlapping areas. Privacy doesn't always rise to the top of those complicated overlapping areas.

So I think Chris is right to ask in general for a kind of resolution of those various pieces of the framework and look at what they're incentivising over time in terms of over-collection and retention for too long. But I suppose what we would bring them back to is the Privacy Act should set a kind of baseline about what good looks like and then, you know, if additional requirements need to be laid on top, well others can make that case. But I think going back, you know, a reset and part of that is about legislative change, but a big part of it is cultural change, I think. Because over the years with all these add on requirements, culturally organisations have become used to just collecting everything and keeping it for as long as they can. And, you know, Scott's exactly right to use that phrase of moving from an asset to a risk. So culturally how do we change attitudes in that way.

Kim Skubris:

And also, I'd imagine as Scott was saying, if it's now identified as a risk, how do we actually get rid of it? How does it, is the footprint there, you know, we always hear that the digital footprint, you really can't erase. Is that fair or not, Chris?

Yeah, look I think what Carly was saying is correct. I think there's a cultural piece of it and businesses looking at information as an asset, because for the most part there are not consequences and I think perhaps we need to be looking at things, like okay, if you wanted to put facial recognition technology into your store, then explain it to us, make sure I've got the option of not going into the store. But then you've got an obligation, as soon as I leave the store, that gets deleted or something like that. Same with the club, I don't know the laws in the clubs, but the fact of the matter is we have laws in the country that assume that every citizen has the potential of engaging in criminal activity. And that cuts against privacy. So we have to be realistic, that if we want to have privacy laws that protect individuals' privacy, we can only do that within a certain framework that says, well, Kim could be a criminal, Paxton could be a criminal, Chris could be a criminal, we could all be criminals and therefore in order for banks or whoever to enable law enforcement to investigate us, they're going to be obliged to collect information on us and our activity. Kind of guilty until proven innocent, so to speak. It's very hard to protect privacy, to the level that we would all expect our privacy to be protected, when you're starting with that baseline. You're really only working in this realm. And there are certain industries, I think, you know, telecommunications, banking, but there's really no reason why a club should be taking photocopies of driver's licences and storing them for seven years or, yeah. So my perspective would be, I think it's time for us to have a fresh, fresh think at some of those laws that are intended to protect us. How do they balance against the right to privacy and human rights.

Carly Kind:

Actually...

Kim Skubris:

You’re nodding away, Paxton.

Paxton Booth:

A recent example is, I think the introduction of guarded carded game play for poker machines and gambling around the state. So we’re starting to see the introduction of laws which require people, so to remove the ability to use cash in gambling. So you’ve got to have a registered card in your name and obviously to get that you’ve got to identify yourself before the card is issued. There's a variety of reasons for introducing those laws around the state. One is anti-money laundering protection, to stop criminals going in and using it to launder their proceeds of crime. The other reason Carly touched upon is about the exclusion list. So some people who have, you know, problems with gambling, want to self-exclude themselves from those venues. So that’s another protection for them. They can go and self-exclude and then, you know, they happen to be at the club one night and having a few drinks, that will actually stop them from getting on the machines and gambling and losing, you know, the family funds.

So it is a bit of a balancing exercise in some regards, but we always, we always look at what is the purpose for collecting the information. Is it, is there a legitimate purpose for collecting the information and are they keeping the collection to a minimum and only keeping it for as long as they really need it. So it really makes, really requires us as the regulators and people in the community to make sure we challenge when people try and collect our information, we don’t understand why. I mean for me, I’d like to have a bit of a call for action for people today around protecting your privacy and one, it’s speaking up, ask people, you know, if they're collecting your personal information, why you're collecting it, and don’t be afraid to say no. You know, if someone’s, particularly in the online environment, if people want a copy of your driver’s licence, say no, or at least ask why and make them actually defend why they're collecting it.

Kim Skubris:

To Scott’s point before though, if you’ve got a bunch of hungry kids and you're standing at a, in a queue in a club and it’s the only place open and they say you're not coming in until you hand over your driver’s licence, what do you do then?

Paxton Booth:

I will be the first to admit, you're not always going to win that argument, but...

Kim Skubris:

Because they want their chicken parmi, and that’s it.

Paxton Booth:

There will be times when you win, and I can certainly talk from my own personal experience since I became Privacy Commissioner, I suppose I've become a bit more aware of protecting my own privacy. And I've gone online to book accommodation and had apps ask me for, you know, all my personal details and upload a copy of your driver's licence, I've just said no, and then there's a phone number down the bottom and I'll call them on the, I've called them up and said look I'm not comfortable providing my driver's licence, oh, that's okay, no worries, well just show it to us when you get here, great. So don't be afraid to challenge and say no.

Kim Skubris:

And I was thinking about when you have someone there new, just walk through the club and show your licence, but again it goes to having an extra person paying the salary. It's that expense as well.

Paxton Booth:

If you've got three hungry kids saying they want to get into the club, that may not be so easy.

Kim Skubris:

This is true, this is true. So in your mind, Paxton, looking forward as Carly said, it's not happening tomorrow, but obviously the continued introduction of AI and technological advancements, would you be able to identify a particular area where you are concerned or excited about the advancement in technology?

Paxton Booth:

Look, I suppose, I'd like to stay on the positive side if I can and one of the areas where I am excited is the digital licences. I think they offer a benefit for all of us in the sense of reducing the impact on our privacy if we can verify our identity online, without having to hand across a copy of our particular driver's licence. I think that's a really potential positive step to help us maintain our privacy in a respectful way. I recently, well not recently, probably 12 months ago now, had an experience at a bank where I had to go and identify myself at a bank. They went away, took my, needed my driver's licence to identify myself, they went away and took a copy of it, left he photocopy on the desk and then the officer left the building, left the office. And then he's like okay, we're all finished up, thanks very much and I went well what are you doing with the copy of my driver's licence just left on top of the desk, he went oh, yeah, we'll get rid of that, and I went well actually would you mind doing it now.

So my concern was when I actually looked over it there was some more copies of other people's driver's licences on the other side of the desk as well, I could still see. So I was making sure that, you know, in those environments when people are actually taking physical copies, they're using, you know, getting rid of it and dealing with it appropriately. The digital verification would have done

away with that entirely and it could have done that through an online and never had to hand across my driver's licence to start with. So I think there are some real benefits in the digital verification scheme, again as long as it's done appropriately.

Kim Skubris:

Chris, what about in your realm through the Queensland Government eyes? What are you embracing that you're excited about or you're being quite cautious about, but need to embrace?

Chris McLaren:

Look on the AI front I'm incredibly optimistic. I think it's a once in a lifetime opportunity. I'm feeling very grateful that I get the opportunity to live through it. If you think about when AI was first conceived, it was, and it's probably 80 years ago now, a group of AI experts, you know, quarantined themselves off for two to three weeks, because they said they were going to solve AI and they literally thought they were two to three weeks away from solving it. And they're all dead, they never got to see it and we're lucky enough that we're here and we get to see it and I think it's fascinating. I think countries like Australia, we've got a huge productivity challenge in front of us. We're lucky to have the benefit of AI to help us solve that productivity challenge as our population ages and we've got less and less young people coming through to do the things that we need them to do. Again, I just go back, we still talk in the language of algorithms when we think of AI, which I think is probably the previous generation of AI language. I think we need to be thinking of the language of models and what do you need to build models, you need data. If we want to make AI behave so to speak or reduce the likelihood that it can misbehave, then we need to focus on the points where all of unnecessary data is being collected and utilised by these models. That's, I think, the focal area that we need to start from.

Kim Skubris:

Where are you adopting this technology from? Is Australia driving a lot of the birth of this technology or where are you bringing in from around the world?

Chris McLaren:

It depends on which part of it. So obviously the large language models are built by the likes of Anthropic and Google and Microsoft open AI, but we don't, we don't have to stop there. So that's kind of like a base model. The analogy I used within Queensland Government a lot, is that we build a product, we call it QChat within Queensland Government. So I describe the model that Microsoft has built or someone, it's like okay, yeah, you've got an exceptionally competent college graduate that's got 25 degrees, 25 advanced degrees in law, engineering, mathematics, physics, blah, blah, blah, but they're still a graduate, they've got no world, real world experience. What we do when we build QChat, is we say right, we've got your college graduate that's got 15 degrees from Harward and all that, what we now need to do now is train them how to be a good Queensland public servant. But then we go through that layer of training with the model, we effectively teach it what Queensland is, what Australia is, see that algorithm?

Kim Skubris:

Do they get a tea break? Like I've got to have my tea break at ten to 10:00, but sorry.

Chris McLaren:

Yeah. What the Public Service Code of Conduct is, what's ethical behaviour and we put it through all that sort of training. We call it safety is a service and then and only then is it ready to act and operate within the confines of the Queensland Public Service. But now that, now that you've got that, I still say to people, so if I was saying to Paxton, you've got access to QChat now, I would say you've got access to it, it's an incredibly powerful resource, but treat it like a super-duper smart college graduate. Are you going to ask a college graduate to write a policy and then give it to the Commissioner or the, no, of course you're not. You're going to say, hey, I need some ideas or write me a draft, or I've got some rough notes or can you do some research on this and then you're going to take accountability for the outcome. So it's a platform that we've got and we're making it available to the public service. We've got, you know, ethics and we've got the, I think the best safety and ethics and AI team in the country. And privacy, cyber security, all of those things are baked in, but you've still got to take ultimate accountability as an individual to how you're using it, just like you would have to take individual accountability if you went out and recruited 15 Harvard graduates, if one of them did something stupid, you know, you're going to say well sorry, my fault, they're new to Queensland Government, they didn't get that you don't say this and you don't do that and they didn't know where Mt Isa was or something. So, you know, that's the level of training that we're putting into the, into the models.

Kim Skubris:

I'm curious, and from a light hearted, keeping it light, not hanging it out to dry, but there must be some interesting anecdotes in the birth of QChat. Can you share something that, as I said not undermining its effectiveness, but was there an interesting...

Carly Kind:

Sounds like it didn't know where Mt Isa was, I think that was the first one that came to, sounded like it didn't know where Mt Isa was. That sounds like a...

Chris McLaren:

No, no, no, not at all.

Kim Skubris:

So is there a story there you can share with us?

Chris McLaren:

It’s the basic things, like if, like under QChat, and someone says who’s the Premier of Queensland, it’s got to be able to say, like I know, like it’s that sort of thing. No, no, no, I just picked Mt Isa out of the hat. I don't know, some of my, the data team are here, they could probably give me some more examples. I mean I used it the other day and all of a sudden it started using American spelling which I'm allergic to having spent so much time in America and I just gave it a thumbs down and said come on, surely, we can get QChat to consistently, you know, use Ss, instead of Zs when it says optimise or whatnot.

Kim Skubris:

(Ui)

Chris McLaren:

But it’s incredibly well behaved and it will, you know, we encourage people to try and break it. We monitor it, we can monitor everything that’s going on. We give agencies the power to monitor it, but this is a tool, because, you know, we had this decision point of AI is here, the toothpaste is out of the tube, what's the best thing we can do as public servants. What would Queensland, Queenslanders expect us to do and I would say learn by doing, doing write policy or regulation from the balcony, get your hands dirty. There’s opportunity here, let’s exploit that opportunity and let’s create a safe space because otherwise people are going to be out there doing M and I(?) and Lama(?) and ChatGPT, which is potentially dangerous. Let’s create a safe space for public servants to operate and use a tool that we can monitor, we can control, it’s got our ethics and safety standards and privacy and cyber security built in and that’s what we've done.

Kim Skubris:

I’m curious, you were sharing then about, I mean we’re talking about Queensland chat, sorry, QChat.

Chris McLaren:

QChat.

Kim Skubris:

It’s almost like it’s got a, I think my kids will joke and say hey, Siri, do you want to marry me and Siri will come back and say I am not the marrying kind and, you know, it’s like, but there's almost this personality that comes into. With QChat you're going to teach QChat where Mt Isa is. There’s this personality. But the more we get into the technological, technological, I won't say that live on television, technological age and AI, are we at risk of losing that empathy? I’ll come through the lens of communication, but the more things are done, you know, through just a data lens and that sort of collection. Scott, do we fear that the good old fashion face to face chat and the, you know, people will forget, actually I'm dealing with a human being, I just see you as a data, you know, extracting

data from you. How important is that that we come back to we are human beings, there has to be that level of empathy and respect for our privacy? So in Privacy Awareness Week, remembering that with all this wonderful technology, we're still talking about human beings and there's that level, I'm saying of empathy as well, about why we should be having our privacy respected.

Scott McDougall

Yeah, and I think we'd all agree that there's enormous potential for technology to improve the lives of people, especially for people living with disability. And, I guess, at the heart of almost all human rights really lies the dignity of the person. And when you, you're talking about that empathy, really it's, it is about a dignity of human beings that we're concerned about when we're talking about human rights. But I do think that there's, you know, there's just so many examples of positive applications of technology. Recently I saw something that Queensland Police are doing, where their body worn camera footage is being reviewed with technology to save the sergeants in the police station all the time of going, reviewing all the footage. So they'll use AI technology to take that sergeant directly to the points of escalation between the officer and the subject in the footage, so that they can go, okay, that's the point that we need to look at, and then they use that for training purposes.

So there are so many potential applications that will improve society. We do have to, we have to harness those, but we have to be, and I probably, we were talking earlier and Chris comes from the private sector and I think it's great that the government's brought you in, Chris, to do your role, because it's exactly what is required. But I read from a regulator lens, I do think we have to be vigilant because we can see it's, I mean there are just so many examples of where if we don't get the regulation right, we do run the risk of, you know, compromising the dignity of people.

Kim Skubris:

And to, I think, because Jo actually, Joanne mentioned this in her share, it is about human rights, and it is about human beings after all. Carly, you'd expand on that from what Scott shared?

Carly Kind:

Yeah, absolutely. I mean I think, just reflecting with Chris was talking, at all times he's talking about QChat as a tool, right, he's saying it is a tool.

It's a tool.

And that's really important I think to avoid that tendency to start to anthropomorphise these technologies and now, you know, some people have a real problem with the term artificial intelligence altogether because it refers, it assumes that this is something approaching humanness, and that's not what we're talking about at all. We're talking about very, very, very smart computers and I think it's really important to distinguish that, but from humans and what we can offer. I really think that the hope and opportunity lies at the intersection of technology and people, and how we really harness that intersection. So whether that be replacing parts of human labour that are boring, repetitive and dangerous and enabling individuals to have safe and more fulfilling roles alongside technology, I think there's real promise and opportunity in that. I think, you reference aging

populations, using technologies in a way that improves their experience, but doesn't replace human contact. I think the idea of carer robots, for example, is pretty horrible to me, but the idea that, you know, older people can connect with their grandchildren and have face to face, human care as well, I think that's what we should be aiming at. So really that intersection of human and, humans and technology is where we should be pointing our lens, I think.

Kim Skubris:

Well, why you have the... Sure, Chris.

Chris McLaren:

I was just going to say that the big, the big space that we're seeing, again back to this productivity dimension, we find a lot of agencies and workforces that are just absolutely overwhelmed, they can't cope with the volume of enquiries or interactions with citizens, businesses. So effectively everybody gets, I'll dramatise it deliberately, the same level of average empathy. Because it's a volume equation. Whereas amongst the 100, let's say interactions, 80 of them, roughly, are probably people with a simple request who just want to get in and get out. It's the 80 that actually need the empathy. So the focus that we often place on the use of technology, if we can use the technology to solve the 80% that just want to get in and get out, then you can dedicate 100% of your empathy on the 20 people who really need it. And we're seeing that across the board. So even though technology is not empathetic, it creates such a productivity uplift that your empathy...

Kim Skubris:

(Ui) time for it.

Chris McLaren:

...is amplified because technology is taking away the burden of those more, those simpler transactions. And it also gives us a mechanism of engaging with citizens. We call it my services, my way. We want citizens to be able to engage with us in a way that they want to engage with us. If they want to engage with us in a text chat, it's like me and you texting over a five-day period, great, well, let them do that if that's what, if they don't want to talk to anybody, if they don't want to go into a counter, we'll have a text conversation. We can do everything we can over a text conversation. If we want them to be able to just do a simple transaction over the phone, perfect. If they want to go into a counter, perfect. It's up to them, versus everybody has to go over here. We get overwhelmed, empathy drops through the floor, and we have to treat everybody the same, because we can't, can't see that that's a simple one, that's a complex one, so giving people choice.

Kim Skubris:

And that would be a perfect world, did you say to amplify the empathy when the nuts and bolts can be done much more quickly. Well in the spirt of giving you all the last say, which is always where I

come from as a moderator and as a host, Paxton, I might start with you. You shared earlier you'd like to reiterate that or share something new, your call to action or your final take away for everybody with Privacy Awareness Week this week.

Paxton Booth:

Yeah, thanks, Kim. As I said I think really my final words are trying to get a call to action out to people, just to challenge the, you know, current collections that are happening and make sure you understand why your information is being collected, whether it be by government agency or a private entity. And don't be afraid to speak up and say no and challenge, challenge.

Kim Skubris:

Thanks, Paxton. Chris.

Chris McLaren:

Yeah, like Paxton stole my line, but I would agree with that. I just think we've got this complacency where if somebody asked for your driver's licence or your date of birth or your mother's maiden name or, we just go, okay, yeah, here you go, here you go, here you go, and I think more and more we need to say, well, why do you need that. But look, I'm incredibly optimistic. I think the potential for us to create better experiences, more private experiences for citizens and businesses, is huge. I am very thankful that I'm alive and I get to do what I do, and I just see bountiful opportunities ahead, noting that we have obligations on us to always put privacy, safety, ethics at the front and centre of everything we do. I should have mentioned before, in QChat and all of our AI work, Paxton actually sits on our advisory group. So we do take this stuff seriously.

Kim Skubris:

Absolutely. Scott.

Scott McDougall:

I actually thought the last question was my closing comment, so.

Kim Skubris:

You want to say what he said and what he said.

Scott McDougall:

Yeah, I'll just say ditto and thank you for the invitation to come tonight. It was a great discussion, thank you, today, not tonight. It's been a long month.

Carly Kind:

It's the 6th of May, isn't it, 7th of May, it's not a good sign.

Kim Skubris:

I was going to say, we have one long weekend and everyone's in go slow zone for the rest of the week. Carly

Carly Kind:

I'm sure everyone's sick of the sound of my voice by now, but I suppose I would say in addition to challenging and taking some individual power back there, I would say don't forget that there is something government can be doing here. So really supporting those moves. I mean I talked a lot about the Privacy Act reform which we hope will be introduced, but they still have to get through parliament and get enacted. So, you know, remember, you know, putting as an individual citizen your political power is important. So putting the support in favour of reform when that time comes.

Kim Skubris:

Well, I'm sure I can speak on behalf of everybody, thank you so much, Carly, Scott, Chris and Paxton. I'm sure everyone who is sharing from around Australia and everyone here, if you'd like to join me. But thank you so much for your time today and for your expertise, it's been really amazing food for thought and certainly I know around our dinner table tonight my two who are all about the Metaverse and AI and one's a budding, an astrophysicist and the other the cricketer, it's like will we come (ui), I go right, what are you sharing and I'll have a few more answers as well this evening. So thank you so much, we really appreciate your time and, on that note, I'd just like to formally conclude today's launch event. Thank you, all. Thank you to Joanne for your share as well, and we truly hope that you really enjoy Privacy Awareness Week and that you've taken some really great advice away from today, and that you go ahead and share it as well. So thank you for your warm welcome from myself as well. Have a great day. Thanks, everyone.

Applause.

Kim Skubris:

Thanks, everyone. Thank you.